HPSR Software Security Content

2015 Update 3

September 30, 2015

HP Software Security Research is pleased to announce the immediate availability of updates to HP Application Defender, HP WebInspect SecureBase (available via SmartUpdate), the HP Fortify Secure Coding Rulepacks (English language, version 2015.3.0), and HP Fortify Premium Content.

About SSR

The Software Security Research team translates cutting-edge research into security intelligence that powers the HP Enterprise Security Products portfolio. Today, HPSR Software Security Content supports 943 vulnerability categories across 22 programming languages and spans more than 832,000 individual APIs.

HP Application Defender

Managed from the cloud, HP Application Defender is a software-as-a-service (SaaS) solution that protects production applications against software security vulnerabilities. For this release, the Software Security Research team provides the following feature improvements:

Dangerous File Inclusion for Java and .NET platforms

- File inclusion allows an attacker to retrieve sensitive files. The attack will now be protected by Fortify whether the file is hosted on the local file system or in a remote location.

HP SecureBase (WebInspect)

HP SecureBase combines checks for thousands of vulnerabilities with policies that guide users in identifying critical weaknesses in web and mobile software.

Vulnerability support

Misconfigured Public Key Pinning

- While certificate pinning thwarts certain cases of man-in-the-middle attacks, missing or misconfigured pinning may give way to hostile attacks. New checks have been added in this release to test for eight different scenarios of misconfiguration to ensure effectiveness of the available protection as per the RFC7496 recommendations.

Misconfigured HTTP Response Headers

- When response headers are misconfigured or incorrectly formatted, browsers interpret them in different and inconsistent ways, thus deviating from the application's intent and potentially violating its security policy. A check has been added to inspect response headers for misconfiguration scenarios subject to browser discrepancies described earlier.

Reflected File Download

- An attacker may exploit improper input handling on websites to entice victims into downloading malicious files that may appear to be hosted on the target site. A new check is available to download via Smartupdate for detecting Reflected File Download in over 30 unique combinations, representing how the vulnerability may manifest, based on the technologies powering the site.

HP Software Security Research
hp.com/go/ssr

SecureBase Enhancements

Source code repository exposure

- Exposure of an application's source code can reveal a treasure trove of information and assist attackers in crafting more sophisticated and targeted attacks against the site. This release includes checks that look for the presence of popular source control directories under the webroot.

Compliance report

PCI DSS v3.1

- The Payment Card Industry (PCI) has updated guidance aligning communication security within the context modern threat scenarios. This release includes a new compliance template to classify and report vulnerabilities according to the PCI v3.1 standard.

HP Fortify Secure Coding Rulepacks (SCA)

With this release, the HP Fortify Secure Coding Rulepacks detect **689** unique categories of vulnerabilities across **22** programming languages and span over **832,000** individual APIs. In summary, the release includes the following:

Spring 4.2 support

- New rulepack enhancements for the latest Spring release, version 4.2, providing support for Spring Web Sockets and Messaging Modules, improving support for Spring Web and the use of Lambda expressions as interface callbacks, and detecting vulnerabilities of the new *Reflected File Download* category within Spring MVC applications.

.NET 4.5.2 APIs

- In support of the latest .NET 4.5.2 APIs, increased rule coverage has been provided for seven existing and nine new namespaces. Additionally, category coverage for *Process Control* has been added for System.AppDomain, as well as *Dynamic Code Evaluation: Code Injection* for System.CodeDom in both C# and VB.NET.

Enhanced Objective-C coverage[1]

- Complementing the new Objective-C translator that shipped with HP Fortify SCA 4.30, rules related to the CoreLocation framework were revised to reflect framework changes introduced with iOS 8.

Python enhancements

- Extended support for Python to include detection of *Memcached Injection* and *Resource Injection* in pylibmc.

PCI DSS 3.1

- Support for the latest Payment Card Industry (PCI) Data Security Standard (DSS) version 3.1.

[1] Requires HP Fortify SCA 4.30.

HP Software Security Research
hp.com/go/ssr

Contact

Joe Sechman
Director, Software Security Research
HP Security Research
sechman@hp.com
+1 (770) 343 -7052

HP Fortify Premium Content

The research team builds, extends, and maintains a variety of resources outside our core security intelligence products.

PCI DSS 3.1 report[2]

- A new report bundle with support for the PCI DSS 3.1 is available for download from the Fortify Customer Portal under Premium Content.

[2] Requires HP Fortify SSC 4.30

Learn more at
hp.com/go/hpsr